

**BY ORDER OF THE COMMANDER
AIR EDUCATION AND TRAINING
COMMAND**



AF INSTRUCTION 14-119

**AIR EDUCATION AND TRAINING COMMAND
Supplement 1**

7 MARCH 2005

Intelligence

INTELLIGENCE SUPPORT TO FORCE PROTECTION (FP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AETC Publishing WWW site at: <http://www.aetc.randolph.af.mil/im>. If you lack access, contact your base publishing manager.

OPR: HQ AETC/DOYIO (Lt Johnny Roper)

Certified by: HQ AETC/DOY (Col Wiley Hill)

Pages: 6

Distribution: F

AFI 14-119, 6 January 2004, is supplemented as follows:

This supplement applies to all Air Education and Training Command (AETC) units and members. It applies to AETC-gained Air National Guard (ANG) and Air Force Reserve Command (AFRC) units and members. Forward requests for waivers to this supplement to HQ AETC/DOYI, identify the specific requirements to be waived and include justification. If approved, a waiver stays in effect for the life of the publication unless HQ AETC/DOYI specifies a shorter period of time, cancels it in writing, or issues a change to the waiver. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with Air Force WebRIMS Records Disposition Schedule (RDS) located at <https://webri.ms.amc.af.mil/rds/index.cfm>. Send suggested improvements to this supplement on AF Information Management Tool (IMT) 847, **Recommendation for Change of Publication**, through command channels to HQ AETC/DOYI, 1 F Street, Suite 2, Randolph AFB, TX 78510-4325.

2.1.2. The AETC senior intelligence officer (SIO) will designate in writing an intelligence professional (at a minimum 14N3 officer, 1N051 NCO, or civilian equivalent) to AETC Threat Working Group (TWG) and AETC Force Protection Working Group (FPWG).

2.1.2.1. Individuals should have appropriate clearance and access to Top Secret (TS), Sensitive Compartmented Information (SCI), HUMINT Control System (HCS), and Gamma (G) data. Cognizant special security office (SSO) must validate access prior to establishing intelligence support to force protection.

3.1. Identify and submit intelligence production requirements (PR) in accordance with AFI 14-105/AETC Sup 1, *Unit Intelligence Mission and Responsibilities*.

3.2.3.1. Through the base TWG provide the commander recommended courses of action to mitigate the threat in accordance with AFI 10-245, *Air Force Antiterrorism (AT) Standards*.

3.2.3.4 Place the appointment memorandum in the AT/FP continuity book and/or electronic folder and forward a copy to HQ AETC/DOYI.

3.2.6. Document intelligence support to FP lessons learned and forward to TWG, FPWG, and HQ AETC/DOYI for action (as required). Maintain lessons learned for future reference. (See Attachment 2 for a checklist of intelligence support to FP.)

3.2.7. All procedures will include support to transient units who previously coordinated current and anticipated intelligence requirements as outlined in AFI 14-105, paragraph 3.5.

3.2.8. Forward all predeployment FP intelligence requirements to HQ AETC/DOYI.

3.2.10. In coordination with the base FPWG, participate in installation vulnerability assessments in accordance with AFI 10-245 and DTRA/USAF VA program guidelines.

3.2.11. Keep one copy of the minutes for each meeting of the TWG in the FP continuity book or electronic folder.

3.2.13. (Added)(AETC) At non-AETC or non-Air Force installations where AETC intelligence units are tenants, the host command (for example, AMC, AFMC, AFSOC, ACC, AFR, ANG) or host service (US Navy, US Army) of the installation is responsible for providing intelligence support to FP for that installation. The AETC intelligence unit should accomplish as a minimum the following:

3.2.13.1. (Added)(AETC) Be familiar with the host base AT/FP plan and/or local supplement, which should detail, if any, their responsibilities to the host unit.

3.2.13.2. (Added)(AETC) Create a continuity book and/or electronic folder and keep all memorandums, requirement statements, and one copy of most recent local FPWG and TWG minutes in it.

3.3.2.3. To the maximum extent possible, identify to HQ AETC/DOYI, inbound personnel who will perform intelligence support to FP duties, and coordinate with HQ AETC/DOYI to arrange for them to attend appropriate FP training enroute to their new duty station.

3.3.2.3.1. (Added) Forward an appointment memorandum to HQ AETC/DOYI with the unit's TWG/FPWG representative (selected from a unit's existing staffing) and coordinate with HQ AETC/DOYI to ensure the representative is properly trained.

4. (Added)(AETC) IMTs Adopted. AF IMT 847, Recommendation for Change of Publication.

NOTE: The following are added to Attachment 1:

References

AFI 10-245/AETC Sup 1, *Air Force Antiterrorism (AT) Standards*

AFI 14-105/AETC Sup 1, *Unit Intelligence Mission and Responsibilities*

GILMARY M. HOSTAGE III, Brigadier General, USAF
Director of Operations

Attachment 2 (Added)(AETC)**INTELLIGENCE SUPPORT TO FORCE PROTECTION**

A2.1. (Added)(AETC) Intelligence Support Checklists. Tables A2.1 (Added)(AETC) through A2.5 (Added)(AETC) provide example checklists.

Table A2.1. (Added)(AETC) In Garrison Checklist.

I T E M	A	B
	Process	Complete
1	Provide significant intelligence related to force protection to OSI and SFS.	
2	Participate in all FPWGs, TWGs, and base defense operations center (BDOC) meetings (real world or exercise).	
3	Conduct internal intelligence training on a semiannual basis or as needed on intelligence support to force protection issues relevant to unit operations (this includes squadron intelligence personnel) to include: - Analytical focus on intelligence message traffic. - Online sites or homepages containing FP data. - Deployed intelligence support to FP responsibilities.	
4	Conduct semiannual external training on intelligence support to force protection issues relevant to unit operations.	
5	Maintain a reference list of intelligence websites or documents related to terrorist and host nation threat data for in garrison and programmed deployment bases. Include: - Mood of local/indigenous population as reported by AFOSI. - Known/identified terrorist groups. - Historical incidents/targeting. - AFOSI assessments on local criminal elements. - Country restrictions. - FPCON levels. - In-place procedures. - Any vulnerability threat assessments from OSI.	
6	Disseminate intelligence related to FP info: - Via read files, web page, and/or message. - Include FP related intelligence issues in CIB regularly or at least quarterly.	
7	Participate and add intelligence value to installation vulnerability assessments during FPWGs and TWGs.	

Table A2.2. (Added)(AETC) Exercise Checklist.

I T E M	A	B
	Process	Complete
	OBJECTIVE: In addition to in-garrison, pre-deployment, employment/sustainment, and redeployment actions the following actions need to be accomplished for local and major exercises.	
1	Coordinate AT/FP threat scenarios with the TWG for realism during exercises.	
2	FEEDBACK: Document intelligence support to FP lessons learned and forward to HQ AETC/DOYI for inclusion into lessons learned databases.	

Table A2.3. (Added)(AETC) Pre-deployment Checklist (If applicable).

I T E M	A	B
	Process	Complete
1	Once unit is identified for possible deployment, monitor AOR events if not already being done.	
2	If it is a short-notice deployment, contact the local AFOSI detachment. - Inform them of possible deployment location and help arrange for unit to receive counterintelligence threat information.	
3	Once deployment location identified, check files and intelligence databases/sources for issues and threats to the deployed locations. - Submit RFIs/PRs as needed to the NAF. - Identify pre-deployment FP requirements to NAF or HQ AETC/DOYI.	
4	Coordinate with TWG to provide commanders with overall assessment.	
5	Ensure all relevant intelligence information is included in unit deployment briefing and/or chalk briefing.	

Table A2.4. (Added)(AETC) Employment/Sustainment Checklist (If applicable).

I T E M	A	B
	Process	Complete
1	Contact onsite SFS and OSI. - Establish FPWG. - Verify the TWG schedule. - Establish intelligence support requirements (maps, charts).	
2	Create and maintain local read files (at appropriate classification levels).	
3	Ensure SIPRNET and JWICS connectivity are established.	
4	Coordinate with local intelligence agencies, to include: - US Embassy (OSI coordination). - Host nation security (OSI coordination). - Other US service organizations (USN, USA, USMC). - Other coalition/multi-national organizations as required.	
5	Ensure intelligence provides FP related intelligence to SFS, OSI, and appropriate commanders in a timely manner.	
6	Contact theater J2/JISE. - Coordinate all FP-related PRs through the J2/JISE or home station if necessary. - Contact J2/JISE minimum three times a week for relevant reports and information. - Work imagery requests through JTF J2/JISE. - J2/JISE should continue to provide data to the FP cell.	
7	Coordinate all intelligence support to FP requirements with the TWG and submit PRs as needed.	
8	Check with local OSI for additional information and reporting.	
9	Ensure deployed unit is receiving intelligence related to FP	
10	Coordinate with local intelligence personnel to ensure: - Read files are updated. - Message traffic includes FP related intelligence. - Updates on local anti-terrorism restrictions and security measures are provided. - Intelligence related to FP are included in current intelligence briefing.	

Table A2.5. (Added)(AETC) Redeployment Checklist (If applicable).

I T E M	A	B
	Process	Complete
1	With the FPWG, coordinate with senior leadership as to exactly when operations and coverage will cease.	
2	FPWG must continue receiving intelligence support until all personnel have departed deployed location: - OSI is still able to obtain information from their sources.	